Secure and reliable connectivity in heterogeneous wireless sensor networks

Rashad Eletreby and Osman Ya˘gan
Department of Electrical and Computer Engineering and CyLab,
Carnegie Mellon University, Pittsburgh, PA, 15213 USA
reletreby@cmu.edu, oyagan@ece.cmu.edu

Abstract—We consider a wireless sensor network secured by a heterogeneous random key predistribution scheme and investigate its reliability against both link and node failures. The heterogeneous random key predistribution scheme is a lightweight security mechanism proposed to secure sensor networks that include nodes with varying levels of resources, features, or connectivity requirements; e.g., regular nodes vs. cluster heads. To capture the reliability of the network against both link and node failures, we consider the case when each link fails independently with probability $1 - \alpha$ and present conditions (in the form of zero-one laws) on how to scale the parameters of the resulting network so that it is $k$-connected with high probability, i.e., the network remains connected even if any $k - 1$ nodes fail or leave the network. Collectively, we obtain a network that is reliable against the probabilistic failure of each link and against the failure of any $k - 1$ nodes. We present numerical results to support these conditions in the finite-node regime.


1. INTRODUCTION

Wireless sensor networks (WSNs) consist of wireless-capable sensor nodes that are typically deployed randomly in large scale and facilitate a broad range of applications including military, health, and environmental monitoring, among others [1]. Most of these applications utilize battery-powered sensors that are required to operate for a long period of time. The low cost of the sensors involved and the stringent requirement on their battery life severely limit the communication and computation capabilities in WSNs. For instance, traditional security mechanisms (e.g., public key cryptography) that require high overhead are not feasible for such resource-constrained networks. However, WSNs are usually deployed in hostile environments and are typically unattended, and thus they require cryptographic protection against adversarial attacks such as node capture, eavesdropping, etc. Random key predistribution schemes were proposed to tackle those limitations, and they are currently regarded as the most feasible solutions in the context of WSNs; e.g., see [2], [3, Chapter 13], and references therein.

Random key predistribution schemes were first introduced in the seminal work of Eschenauer and Gligor [4]. Their scheme, referred to as the EG scheme, operates as follows: before deployment, each sensor node is assigned a set of $K$ cryptographic keys selected uniformly at random from a key pool of size $P$. After deployment, a pair of nodes can communicate securely only if they share at least one key. The EG scheme led the way to several other variants, including the $q$-composite scheme [5], the random pairwise scheme [5], [6], and many others.

Recently, Ya˘gan [7] introduced a new variation of the EG scheme, referred to as the heterogeneous key predistribution scheme. As the name suggests, their approach generalizes the EG scheme to accommodate applications that contain sensors with varying level of resources, capabilities, and connectivity/security requirements; e.g., regular nodes vs. cluster heads. It is in fact envisioned that many real-world implementations of WSNs will be heterogeneous [8]. The heterogeneous scheme operates as follows: Before deployment, each sensor is independently assigned to one of $r$ priority classes, with $\mu_i > 0$ denoting the probability of being assigned to class-$i$, for each $i = 1, \ldots, r$. Each class-$i$ sensor is then given $K_i$ cryptographic keys selected uniformly at random from a key pool of size $P$. Similar to the EG scheme, only sensors that share key(s) can establish a secure communication link after the deployment; see Section 2 for details.

The main contribution of [7] was to demonstrate the feasibility of the heterogeneous scheme by showing how its parameters can be selected such that, after deployment, there is a secure communication path between every pair of sensors. This was done by studying the connectivity of a random graph model induced naturally under the heterogeneous scheme. With $K = \{K_1, K_2, \ldots, K_r\}$, $\mu = \{\mu_1, \mu_2, \ldots, \mu_r\}$, and $n$ denoting the network size, let $E(n; \mu, K, P)$ denote the random graph, defined on vertices $\{v_1, \ldots, v_n\}$, where any pair of nodes are adjacent as long as they share a key. This graph is referred to as the inhomogeneous random key graph [7], and generalizes the well-studied (homogeneous) random key graph model induced under the EG scheme [9], [10]. Since then, the work on the heterogeneous scheme has been extended in several directions by the authors; e.g., see [11]–[14].

The objective of this paper is to investigate the reliability of the heterogeneous key predistribution scheme against both link and node failures. In particular, we consider a WSN secured by the heterogeneous key predistribution scheme and examine the probability of the network remaining connected despite i) the probabilistic failure of each wireless link connecting sensor nodes and ii) the failure of a finite number of sensor nodes. Indeed, real-world WSNs are vulnerable to link and node failures for many reasons. For instance, wireless links are prone to failure due to interference, multipath fading, shadowing, among
other phenomenas caused by the randomness of the wireless channel. Moreover, sensor nodes are susceptible to physical damage, battery depletion [15], and node capture attacks [5]. Such scenarios may cause the disconnection of the network, preventing the flow of critical information between sensor nodes, and rendering the network unreliable. The preceding discussion brings about a very crucial question: How can we adjust the parameters of the heterogeneous key predistribution scheme, namely, $\mu$, $K$, and $P$, in a way that guarantees the reliability of the network against link and node failures? Our paper answers this question by means of presenting conditions (in the form of zero-one laws) on how to scale the parameters of the heterogeneous key predistribution scheme (relative to the network size $n$) such that the resulting network is both secure and reliable with high probability as $n$ gets large.

In [12], a crucial first step towards investigating the reliability of WSNs under the heterogeneous scheme was completed. In particular, with an eye towards modeling the unreliability of wireless links, we considered the graph $\mathcal{H}(n, \mu, K, P, \alpha)$ obtained by deleting each edge of $\mathbb{K}(n, \mu, K, P)$ independently with probability $1 - \alpha$. We then established conditions on the parameters of $\mathcal{H}(n, \mu, K, P, \alpha)$ such that its minimum node degree is no less than $k$, for any arbitrary integer $k$. This property provides some notion of reliability against sensor failures (in addition to probabilistic link failures) in that every node would have at least one neighbor even if any $k - 1$ sensors fail. However, it does not provide any guarantee on the network remaining connected in the face of sensor failures. The current paper fills this gap by establishing conditions for the $k$-connectivity of $\mathcal{H}(n, \mu, K, P, \alpha)$; i.e., conditions that would ensure that the graph will remain connected despite the failure of any $k - 1$ nodes. In fact, it was conjectured in [12, Conjecture 3.2], that under some additional conditions, the zero-one laws for $k$-connectivity would resemble those given in [12] for the minimum node degree being no less than $k$. Our main result (see Theorem 3.1) proves this conjecture and provides the extra conditions needed for it to hold.

In addition to ensuring that the resulting WSN will be reliable against the probabilistic failure of each link and the failure of any set of $k - 1$ sensors, the $k$-connectivity of $\mathcal{H}(n, \mu, K, P, \alpha)$ leads to some other desirable network properties. For instance, it ensures that any pair of nodes have $k$ mutually disjoint paths connecting them [16], providing communication reliability when sensors operate autonomously and physically unprotected; e.g., as long as one of the $k$ paths between them are not compromised by the adversary, a pair of sensors can transfer messages between each other. Alternatively, $k$-connectivity may enable assigning any $k - 1$ sensors as mobile nodes that can roam around anywhere in the network (thereby forming and removing edges), while the whole WSN remains connected; e.g., see [17].

We close with a word on notation and conventions in use. All limiting statements, including asymptotic equivalences are considered with the number of sensor nodes $n$ going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$.

Probabilistic statements are made with respect to this probability measure $\mathbb{P}$. We say that an event holds with high probability (whp) if it holds with probability 1 as $n \to \infty$. In comparing the asymptotic behaviors of the sequences $\{a_n\}, \{b_n\}$, we use $a_n = o(b_n)$, $a_n = \omega(b_n)$, $a_n = O(b_n)$, $a_n = \Omega(b_n)$, and $a_n = \Theta(b_n)$, as per the standard Landau notation.

2. The Model

We consider a network consisting of $n$ sensor nodes labeled as $v_1, v_2, \ldots, v_n$. Each node is assigned to one of the $r$ possible classes according to a probability distribution $\mu = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for each $i = 1, \ldots, r$ and $\sum_{i=1}^{r} \mu_i = 1$. Before deployment, a class-$i$ node selects $K_i$ cryptographic keys uniformly at random from a key pool of size $P$. In other words, the key ring $\Sigma_v$ of node $v_i$ is a $\mathcal{P}_{K_i}$-valued rv where $\mathcal{P}_{K_i}$ denotes the collection of all subsets of $\{1,\ldots,P\}$ with exactly $K_i$ elements and $t_x$ denotes the class of node $v_x$. The rvs $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ are then i.i.d. with

$$\mathbb{P}[\Sigma_x = S \mid t_x = i] = \binom{P}{K_i}^{-1}, \quad S \in \mathcal{P}_{K_i}.$$  

After deployment, two nodes that have at least one key in common can communicate securely.

Throughout, we let $K = \{K_1, K_2, \ldots, K_r\}$, and assume without loss of generality that $K_1 \leq K_2 \leq \ldots \leq K_r$. Consider a random graph $\mathbb{K}$ induced on the vertex set $V = \{v_1, \ldots, v_n\}$ such that distinct nodes $v_x$ and $v_y$ are adjacent, denoted by the event $K_{xy}$, if they have at least one key in common, i.e.,

$$K_{xy} := [\Sigma_x \cap \Sigma_y \neq \emptyset].$$

(1)

The adjacency condition (1) describes the inhomogeneous random key graph $\mathbb{K}(n; \mu, K, P)$ that has been introduced in [7]. This model is also known in the literature as the general random intersection graph; e.g., see [18]–[20].

The inhomogeneous random key graph models the secure connectivity of the underlying WSN. In particular, the probability $p_{ij}$ that a class-$i$ node and a class-$j$ have a common key, and thus are adjacent in $\mathbb{K}(n; \mu, K, P)$, is given by

$$p_{ij} = \mathbb{P}[K_{xy}] = 1 - \frac{\left(\frac{P - K_i}{K_j}\right)}{\left(\frac{P}{K_j}\right)}$$

(2)

as long as $K_i + K_j \leq P$; otherwise if $K_i + K_j > P$, we clearly have $p_{ij} = 1$. The mean probability of edge occurrence for a class-$i$ node in $\mathbb{K}(n; \mu, K, P)$, denoted $\lambda_i$, is given by

$$\lambda_i = \sum_{j=1}^{r} p_{ij} \mu_j, \quad i = 1, \ldots, r.$$  

(3)

Our objective is to investigate the reliability of the inhomogeneous random key graph $\mathbb{K}(n; \mu, K, P)$ against both link and node failures. To this end, we assume that each edge in $\mathbb{K}(n; \mu, K, P)$ fails independently with probability $1 - \alpha$ and study the probability that the resulting graph is $k$-connected. Namely, we consider the graph $\mathcal{H}(n; \mu, K, P, \alpha)$ formed by deleting each edge of $\mathbb{K}(n; \mu, K, P)$ independently with probability $1 - \alpha$. Then, we derive conditions on how to
scale the parameters $K, P, \alpha$ with the network size $n$, such that $H(n; \mu, K_n, P_n, \alpha_n)$ is $k$-connected with high probability as $n$ gets large. The $k$-connectivity implies that the graph remains connected even if any $k - 1$ nodes are deleted. Thus, the $k$-connectivity of $H(n; \mu, K_n, P_n, \alpha_n)$ implies that the WSN remains securely connected despite i) the failure of each link with probability $1 - \alpha$ and ii) the failure of any $k - 1$ sensors.

To simplify the notation, we let $\theta = (K, P)$, and $\Theta = (\theta, \alpha)$. The probability of edge existence between a class-$i$ node $v_x$ and a class-$j$ node $v_y$ in $H(n; \Theta)$ is given by

$$P[E_{xy} \mid t_x = i, t_y = j] = \alpha p_{ij}$$

by independence. Similar to (3), the mean edge probability for a class-$i$ node in $H(n; \mu, \Theta)$, denoted by $\lambda_i$, is given by

$$\lambda_i = \sum_{j=1}^{r} \mu_j \alpha p_{ij} = \alpha \lambda_i, \quad i = 1, \ldots, r. \quad (4)$$

From now on, assume that the number of classes $r$ is fixed and does not scale with $n$, and so are the probabilities $\mu_1, \ldots, \mu_r$. All of the remaining parameters are assumed to be scaled with $n$.

3. MAIN RESULT AND DISCUSSION

A. Result

We refer to a mapping $K_1, \ldots, K_r, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0^{r+1}$ as a scaling (for the inhomogeneous random key graph) as long as the conditions

$$2 \leq K_{1,n} \leq K_{2,n} \leq \cdots \leq K_{r,n} \leq P_n/2 \quad (5)$$

are satisfied for all $n = 2, 3, \ldots$. Similarly any mapping $\alpha : \mathbb{N}_0 \rightarrow (0, 1)$ defines a scaling for $\alpha$. As a result, a mapping $\Theta : \mathbb{N}_0 \rightarrow \mathbb{N}_0^{r+1} \times (0, 1)$ defines a scaling for $H(n; \mu, \Theta_n)$ given that condition (5) holds. We remark that under (5), the edge probabilities $p_{ij}$ will be given by (2), and we have

$$\lambda_1(n) \leq \lambda_2(n) \leq \cdots \leq \lambda_r(n)$$

for all $n = 2, 3, \ldots$.

We now present a zero-one law for the $k$-connectivity of $H(n; \mu, \Theta_n)$.

**Theorem 3.1.** Consider a probability distribution $\mu = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\Theta : \mathbb{N}_0 \rightarrow \mathbb{N}_0^{r+1} \times (0, 1)$. Let the sequence $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ be defined through

$$\lambda_1(n) = \alpha_n \lambda_1(n) = \frac{\log n + (k - 1) \log \log n + \gamma_n}{n}, \quad (6)$$

for each $n = 1, 2, \ldots$. 

(a) If $\lambda_1(n) = o(1)$, we have

$$\lim_{n \rightarrow \infty} P[H(n; \mu, \Theta_n) \text{ is } k\text{-connected}] = 0 \quad \text{if} \quad \lim_{n \rightarrow \infty} \gamma_n = -\infty$$

(b) If $P_n = \Omega(n), \frac{K_{r,n}}{P_n} = o(1), \frac{K_{r,n}}{\alpha} = o(\log n)$, we have

$$\lim_{n \rightarrow \infty} P[H(n; \mu, \Theta_n) \text{ is } k\text{-connected}] = 1 \quad \text{if} \quad \lim_{n \rightarrow \infty} \gamma_n = \infty.$$
against link failure, but do not provide any indication on whether the network would remain connected when one or more nodes fail. Such a limitation renders the result in [11] incapable of facilitating the cases when sensor nodes fail due to battery depletion, get captured by an adversary, etc. Therefore, sharper results that guarantee network connectivity in the aforementioned scenarios are needed.

Our paper broadens the scope of the results given in [11]. In particular, by considering the $k$-connectivity property of $H(n; \mu, K, P)$ (in contrast to the 1-connectivity property considered in [11]), we ensure that the network would remain connected even if any $k - 1$ nodes fail. In sum, we obtain a network that is both reliable against the probabilistic failure of each link and also against the failure of any $k - 1$ nodes. Indeed, by setting $k = 1$ and $\gamma_n = (c - 1) \log n$ in Theorem 3.1, our results get reduced to the results given in [11]. We refer the reader to [21] for an extensive discussion on related work.

4. Numerical Results

In this section, we present numerical results to support Theorem 3.1 in the finite node regime. In all experiments, we fix the number of nodes at $n = 500$ and the size of the key pool at $P = 10,000$. To help better visualize the results, we use the curve fitting tool of MATLAB.

In Figure 1, we consider the reliability parameters $\alpha = 0.2$, $\alpha = 0.4$, $\alpha = 0.6$, and $\alpha = 0.8$, while varying the parameter $K_1$, i.e., the smallest key ring size, from 5 to 40. The number of classes is fixed to 2, with $\mu = \{0.5, 0.5\}$. For each value of $K_1$, we set $K_2 = K_1 + 10$. For each parameter pair $(K_1, \alpha)$, we generate 200 independent samples of the graph $H(n; \mu, \Theta)$ and count the number of times (out of a possible 200) that the obtained graphs are 2-connected. Dividing the counts by 200, we obtain the (empirical) probabilities for the event of interest.

In Figure 1 as well as the ones that follow we show the critical threshold of connectivity “predicted” by Theorem 3.1 by a vertical dashed line. More specifically, the vertical dashed lines stand for the minimum integer value of $K_1$ that satisfies

$$\lambda_1(n) = \sum_{j=1}^{2} \mu_j \left( 1 - \frac{(P - K_1/K_2)}{P} \right) > \frac{1}{\alpha} \log n + (k - 1) \log \log n$$

with any given $k$ and $\alpha$. We see from Figure 1 that the probability of $k$-connectivity transitions from zero to one within relatively small variations in $K_1$. Moreover, the critical values of $K_1$ obtained by (8) lie within the transition interval.

In Figure 2, we consider four different values for $k$, namely we set $k = 4$, $k = 6$, $k = 8$, and $k = 10$ while varying $K_1$ from 15 to 40 and fixing $\alpha$ to 0.4. The number of classes is fixed to 2 with $\mu = \{0.5, 0.5\}$ and we set $K_2 = K_1 + 10$ for each value of $K_1$. Using the same procedure that produced Figure 1, we obtain the empirical probability that $H(n; \mu, \Theta, \alpha)$ is $k$-connected versus $K_1$. The critical threshold of connectivity asserted by Theorem 3.1 is shown by a vertical dashed line in each curve. Again, we see that numerical results are in parallel with Theorem 3.1.

Figure 3 is generated in a similar manner with Figure 1, this time with an eye towards understanding the impact of the minimum key ring size $K_1$ on network connectivity. To that end, we fix the number of classes at 2 with $\mu = \{0.5, 0.5\}$ and consider four different key ring sizes $K$ each with mean 40; we consider $K = \{10, 70\}$, $K = \{20, 60\}$, $K = \{30, 50\}$, and $K = \{40, 40\}$. We compare the probability of 2-connectivity in the resulting networks while varying the link failure probability $1 - \alpha$ from zero to one. We see that although the average number of keys per sensor is kept constant in all four cases, network connectivity improves dramatically as the minimum key ring size $K_1$ increases; e.g., with $1 - \alpha = 0.8$, the probability of connectivity is one when $K_1 = K_2 = 40$ while it drops to zero if we set $K_1 = 10$ while increasing $K_2$ to 70 so that the mean key ring size is still 40.

Finally, we examine the reliability of $H(n; \mu, \Theta, \alpha)$ by looking at the probability of 1-connectivity as the number of deleted (i.e., failed) nodes increases. From a mobility
This work has been supported in part by National Science Foundation through grant CCF-1617934.

ACKNOWLEDGMENT

This work has been supported in part by National Science Foundation through grant CCF-1617934.

REFERENCES


